JOURNAL OF ALGEBRA 27, 306–310 (1973)

On the Commutator Subgroups of Certain Unitary Groups

C. T. C. WALL

Department of Mathematics, University of Liverpool, Liverpool, England

Communicated by J. Tits

Received February 29, 1972

Let G be a classical group, i.e., [8] for some field K, central simple algebra A of finite dimension over K, and (anti-) involution α of A, $G = \{x \in A: x^\alpha x = 1\}$. Then it is wellknown (for references see [3, Chapter II]) that, with a handful of small exceptions, if α has index $\nu \geqslant 1$, and T is the subgroup of G generated by transvections then T modulo its center ($= G \cap K$) is simple.

It is less easy to identify the subgroup T; the results depend on α. If α is of symplectic type, then $T = G$ [3, p. 48]. If α is of unitary type, and A is trivial (i.e., a matrix ring over K), then (with one exception) T is the subgroup of G of matrices with determinant 1 [3, p. 49]. If α is of orthogonal type, and A is trivial, we can detect the quotient G/T by determinant and spinor norm.

The case when A is a matrix ring over a noncommutative division ring D is less well understood. If K is a local or global field, and α has orthogonal type, then D must be a quaternion ring. The corresponding result here has been proved by M. Kneser using induction and an exceptional isomorphism. This leaves only the case, D noncommutative and α of unitary type (or "of the second kind"). This case does not arise over local fields K. We will show the following.

THEOREM 1. *Let K be an algebraic number field, A a central simple algebra of finite dimension at least nine over K, α an (anti-) involution of A of the second kind and of nonzero index. Then T is the subgroup of G of elements of reduced norm* 1.

In a natural notation, T is the corresponding special unitary group SU. Thus our result is equivalent to saying that the groups SU are simple. Since SU is a 1-connected algebraic group, our result also supports the conjecture that any such group of index $\geqslant 1$ (i.e., isotropic) is generated by 1-parameter subgroups isomorphic (as algebraic groups) to the additive group of the field. For transvections lie in such subgroups. This result, for arbitrary fields, has been announced by Platonov.

The proof of Theorem 1 depends on some results of Wall [6] (see also [3, pp. 47–48]) which for our purpose can be formulated as follows. We can write $A = M_n D$, D a division ring, and take α as conjugate transpose with respect to some antiinvolution, also denoted α, of D. Let Σ denote the set of nonzero symmetric elements of D. According to Wall, under our assumptions, there is an isomorphism

$$N : G/T \to D^\times/\Sigma[D^\times, D^\times].$$

We compare this with the reduced norm *Nrd*, which is certainly trivial on T, and takes values in $K^\times$. By a result of Wang [7], *Nrd* induces an injective map

$$Nrd : D^\times/[D^\times, D^\times] \to K^\times.$$

The definition of N involves expressing an element of G as product of "symmetries" s_i, and giving $N(s_i)$ explicitly.

We find, by inspection for the s_i, and hence for any $g \in G$, that for some (hence all) $d \in D^\times$ representing $N(g)$, we have

$$Nrd\, g = Nrd(dd^{-\alpha}).$$

Thus, if $Nrd\, g = 1$, $Nrd\, d$ is a symmetric element of $Nrd\, D^\times \subset K^\times$. If we can show that all such elements belong to the subgroup generated by $Nrd\, \Sigma$ it will follow that, modulo Σ, we have $Nrd\, d = 1$, i.e., $d \in [D^\times, D^\times]$, and, thus, that $N(g) = 1$, so by Wall's result, $g \in T$. Thus, Theorem 1 will follow from the following theorem.

THEOREM 2. *Let K be an algebraic number field, D a central division ring of finite dimension over K, α an anti-involution of D of the second kind, Σ the symmetric elements of D. Then any element of $Nrd\, D^\times$ which is α-symmetric belongs to the subgroup generated by $Nrd\, \Sigma$.*

The result seems to depend on the explicit form of α; the last paragraph of the proof, however, can be adapted to show directly that $Nrd\, \Sigma$ is unaltered by replacing α by an equivalent antiinvolution. We regard the result as a refinement of Eichler's (see e.g. [9]) computation of $Nrd\, D^\times$, and our proof parallels his. Compare also [4, Proposition 1b, p. 103].

LEMMA 1. *Let K be a p-adic local field, $\lambda \neq 0$ in K, $n > 0$ an integer. There exists an irreducible monic polynomial over K, of degree n, with constant term $(-1)^n\lambda$.*

Proof. Let $v: K^\times \to \mathbf{Z}$ be the valuation, π a prime, i.e., $v(\pi) = 1$. Let d be the h.c.f. of n and $v(\lambda)$: write $n = rd$, $v(\lambda) = wd$. Then $\pi^{-wd}\lambda$ is a unit; hence, [9, Lemma 2, p. 208] if K_1 is e.g. the Abelian unramified extension of

K of degree d, we have $K_1 = K(y)$ with $N(y) = (-1)^{n-d}\pi^{-wd}\lambda$. Let f be the minimal polynomial of $\pi^w y$: f is then irreducible. Since w and r are coprime, $x^r - \pi^w y$ is irreducible over K_1 (any root generates a totally ramified extension of degree r). It follows by a theorem of Capelli [2][1] that $f(x^r)$ is irreducible over K: this polynomial has the desired properties.

LEMMA 2. *Let K be a quadratic extension of the algebraic number field k; let S be a finite set of finite primes of k which decompose in K; let $\lambda \neq 0$ in k and $n > 0$ be an integer. There exists a monic polynomial f of degree n over k with constant term $(-1)^n\lambda$ such that*

(1) *f is irreducible over each $k_\mathfrak{p}$, $\mathfrak{p} \in S$;*

(2) *f is irreducible over K;*

(3) *if n is even, we may suppose f has no real roots at any real place of k at which $\lambda > 0$.*

Proof. If S is nonempty, (2) follows from (1), for $k_\mathfrak{p}$ is an extension of K. As there are always decomposed primes, we can enlarge S to be nonempty.

For each $\mathfrak{p} \in S$, choose a polynomial

$$x^n + a_{1,\mathfrak{p}}x^{n-1} + \cdots + a_{n-1,\mathfrak{p}}x + (-1)^n\lambda$$

over $k_\mathfrak{p}$ as in Lemma 1. If n is even, we also choose

$$x^n + (-1)^n\lambda \qquad \text{(i.e., } a_{i,\mathfrak{p}} = 0\text{)}$$

at each real place of k. By the weak approximation theorem, there exist $a_i \in k$ with

$$\| a_i - a_{i,\mathfrak{p}} \|_\mathfrak{p}$$

arbitrarily small for each i, $1 \leqslant i < n$ and $\mathfrak{p} \in S$ or real. But now as on [9, p. 209], it follows from his Lemma 1 that if the approximation is sufficiently close, the polynomial

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + (-1)^n\lambda$$

will have the stated properties.

LEMMA 3. *Let K be an algebraic number field, D a central division algebra over K with $\dim_K D = n^2$, α an antiinvolution of D whose restriction to K has fixed field $k \neq K$. Let $\lambda \in k$ be positive at each real place of k where D is ramified. Then there is a monic irreducible polynomial f of degree n over k,*

[1] I am indebted to Dr. M. C. R. Butler for suggesting the use of this result.

with constant term $(-1)^n\lambda$, *such that if* $l = k(z)$ *is generated by a root of* f, *then* $L = Kl$ *is a field and there is a* K*-embedding* $e: L \to D$.

Proof. Since α is of the second kind (has $k \neq K$), each prime of K where D is ramified is decomposed for K/k.[2] Let S be the corresponding set of primes of k. Let f be as given by Lemma 2. Since f is irreducible over K, L is a field.

We next show that L splits D. By the calculation of BrK, it follows that it is enough to see this locally. The finite localisations of K where D is ramified are, by construction, inert for L/K. Now as $\dim_K D = n^2$, by [5, Corollary 3, p. 202] the corresponding element to $D_\mathfrak{p}$ of $Br(K_\mathfrak{p})$ has order dividing n, and is split by the extension $L_\mathfrak{p}$ of $K_\mathfrak{p}$ of degree n. At any real prime of K where D ramifies $\lambda > 0$ by hypothesis. By Lemma 2, f has no real roots, so again the extension splits D.

Thus, L splits D; now as on [9, p. 210] it follows from [9, Corollary 3, p. 180] that an embedding e exists.

LEMMA 4. *Suppose* K, D, α, n, k *as in Lemma* 3, *and* l *an extension of degree* n *of* k *such that* $L = Kl$ *is a field admitting a* K*-embedding* $e: L \to D$. *Then there exists* $y \in D$, $y \neq 0$, *with* $y^\alpha = y$ *such that if* β *is the involution of* L/l, $e(x^\beta) = y^{-1}e(x)^\alpha y$ *for all* $x \in L$.

Proof. We define another K-embedding of L in D by $x \mapsto e(x^\beta)^\alpha$. By the Skolem–Noether theorem, this is conjugate to e: say $e(x^\beta)^\alpha = w^{-1}e(x)w$ for all $x \in K$. Thus, $e(x^\beta) = w^\alpha e(x)^\alpha w^{-\alpha}$. It thus will suffice to find $b \in L$ such that $y = e(b)^\alpha w^{-\alpha}$ satisfies $y^\alpha = y$.

Now $e(x) = e(x^{\beta\beta}) = w^\alpha e(x^\beta)^\alpha w^{-\alpha} = w^\alpha w^{-1}e(x)\, ww^{-\alpha}$ for all $x \in L$, so $w^\alpha w^{-1}$ commutes with $e(L)$ which, for dimensional reasons, is a maximal commutative subring. Hence, $w^\alpha w^{-1} = e(c)$ for some $c \in L$. I claim $c^\beta c = 1$. For $e(c^\beta c) = w^\alpha e(c)^\alpha w^{-\alpha} w^\alpha w^{-1} = w^\alpha w^{-\alpha} ww^{-1} = 1$. It follows from the Hilbert Satz 90 that we can write $c = b^\beta b^{-1}$ for some $b \in L$ (if $c \neq -1$, we can simply take $b = 1 + c^\beta$). Now defining y as above,

$$\begin{aligned} y^\alpha y^{-1} &= w^{-1}e(b)\, w^\alpha e(b)^{-\alpha} = w^{-1}e(b)(w^{-1}e(b^{-1})w)^\alpha w^\alpha \\ &= w^{-1}e(b)\, e(b^{-\beta})\, w^\alpha = w^{-1}e(c^{-1})\, w^\alpha \\ &= w^{-1}wzw^{-\alpha}w^\alpha = 1. \end{aligned}$$

Proof of Theorem 2. Let λ be an α-symmetric element of $Nrd\, D^\times$,—i.e., $\lambda \in k$, $\lambda \neq 0$, and $\lambda > 0$ at real primes where D ramifies. By Lemma 3 we

[2] For if not, we would have an involution on a nontrivial algebra over $K_\mathfrak{p}$, whence one can easily obtain one on a quaternion division ring over $K_\mathfrak{p}$. But this contradicts a theorem of Albert [1]. A more detailed version of this argument appears in [4, p. 40].

can construct an extension $l = k(z)$ of degree n, with $N_{l/k}z = \lambda$, such that $L = Kl$ is a field, and there is a K-embedding $e: L \to D$. By Lemma 4, there exists $y \in D^\times$ with $y^\alpha = y$ and $e(x^\beta) = y^{-1}e(x)^\alpha y$ for all $x \in L$, where β is the involution of L/l. Then as $z \in l$,

$$(ye(z))^\alpha = e(z)^\alpha y^\alpha = yy^{-1}e(z)^\alpha y = ye(z^\beta)) = ye(z)$$

so $ye(z)$, as well as y, is symmetric.

Now $\lambda = N_{l/k}(z) = N_{L/K}(z)$ and by [9, p. 179] this equals $Nrd\, e(z)$. But $e(z)$ is the product of the α-symmetric elements y^{-1} and $ye(z)$, so the proof is complete.

References

1. A. A. Albert, "Structure of Algebras," Amer. Math. Soc., Providence, RL, 1939.
2. A. Capelli, Sulla riduttibilità delle equazioni algebriche, *Rendiconti Accad. Sci. Napoli* **IV** (1898), 84–90.
3. J. Dieudonné, "La géométrie des groupes classiques," second ed., Springer, Berlin, 1963.
4. M. Kneser, "Galois Cohomology of Classical Groups," Tata Institute, Bombay, 1972.
5. J.-P. Serre, "Corps Locaux," Hermann, Paris, 1962.
6. G. E. Wall, The structure of a unitary factor group, *Publ. Math. I.H.E.S.* 1 (1959).
7. S. Wang, On the commutator group of a simple algebra, *Amer. J. Math.* **72** (1950), 323–334.
8. A. Weil, Algebras with involutions and the classical groups, *J. Indian Math. Soc.* **24** (1961), 589–623.
9. A. Weil, "Basic Number Theory," Springer, Berlin, 1967.